UNITED STATES MARINE CORPS
III MARINE EXPEDITIONARY FORCE, FMF
FPO SAN FRANCISCO, CA 96606-8400

IN REPLY REFER TO:
ADJ
25 May 90

ERRATUM

TO

FORO 5239.1

AUTOMATED DATA PROCESSING (ADP)
SECURITY PROCEDURES

1. The entire Order was reproduced erroneously. Upon receipt remove the current Force Order 5239.1 in its' entirety and replace with the corrected Order hereto attached.

DISTRIBUTION: List I/II

UNITED STATES MARINE CORPS
III MARINE EXPEDITIONARY FORCE, FMF
FPO SAN FRANCISCO, CA 96606-8400

ForO 5239.1
ISMO
29 Apr 90

FORCE ORDER 5239.1

From: Commanding General
To: Distribution List

Subj: AUTOMATED DATA PROCESSING (ADP) SECURITY PROCEDURES

Encl: (1) Guidance for Automated Data Processing Security Procedures

1. Purpose. To establish an ADP security program.

2. Background. Microcomputers and word processing equipment exist in virtually every office and work space in the western Pacific. This end user computing equipment (EUCE) enhances our ability to perform daily administrative functions. EUCE also creates additional consideration for the security manager and user when processing sensitive and/or classified information.

3. Action. Commanders will ensure the contents of this order are included in the routine indoctrination process of all individuals.

4. Effective Date. 31 July 1990

H. F. GOTARD
Chief of Staff

DISTRIBUTION: List I/II

GUIDANCE FOR AUTOMATED DATA PROCESSING SECURITY PROCEDURES

1. POLICY AND RESPONSIBILITY.

a. Policy. Automated Data Processing (ADP) security is an extension of normal information security policy and procedures set forth in other orders. All personnel will receive, as part of the security indoctrination, specific guidance relative to the use of computers. The security procedures normally applied to manual and paper systems apply equally to computer based systems. This order provides added guidance on the use and handling of all word processing equipment, desktop/portable microcomputer systems, on-line terminals, and the Fleet Marine Force-End User Computing Equipment (FMF-EUCE) machines. A glossary of ADP terms is included at appendix A.

b. Responsibilities. Commanders have overall responsibility for ADP security. They will ensure the following billets are filled and that adequate programs exist to comply with this directive and applicable orders of higher headquarters.

(1) Security Manager. The Security Managers are responsible to the Commanding Officer for management of the Information and Personnel Security Program. They are guided in their duties by OPNAVINST 5510.1F which encompasses aspects of ADP security.

(2) Assistant Chief of Staff, G-6/ISMO. The G-6/ISMOs have staff cognizance over all ADP security matters. They are responsible for coordinating ADP security matters with the security manager and directing the activities of their ADP security officers. They will ensure that EUCE security, as defined by this order, is fully implemented.

(3) Automated Data Processing Security Officer (ADPSO). The Automated Data Processing Security Officers are action officers for the Assistant Chief of Staff, G-6/ISMO in all matters pertaining to ADP security. The ADPSOs coordinate with the various staff sections advising and assisting them in implementing ADP security requirements of the section. They provide/coordinate ADP security training for the command according to the guidelines of appendix B and, through the G-6/ISMO, are the command's focal point in matters relating to emission security (TEMPEST) requirements. ADPSOs will be granted in their duties by this order, OPNAVINST 5239.1A, and OPNAVINST C5510.93E.

(4) Automated Data Processing Section Security Assistant (ADPSSA). Each organization within III MEF shall appoint in writing an ADPSSA who shall assist the Automated Data Processing Security Officer in the performance of their duties by:

(a) Ensuring all computer systems are accredited in accordance with procedures outlined in this enclosure.

(b) Ensuring that all systems are properly marked and have the warning screen software installed.

(c) Maintaining a current inventory of all assigned computer equipment and software assigned to the section.

(d) Developing and/or maintaining ADP Security Standard Operating Procedures (SOP) and contingency plan.

(e) Serving as the point of contact for all ADP security matters.

(f) Maintaining a current list of passwords and control access to section computer equipment.

2. PROCEDURES. The procedures for handling and processing classified information on ADP equipment are generally the same as those for typing classified information on a typewriter. Diskettes and other magnetic storage devices often contain classified data.

3. COMPUTER SYSTEM ACCREDITATION. Accreditation is the formal statement by a Designated Approving Authority (DAA) declaring that all known vulnerabilities and risks associated with a computer system have been considered and prudent countermeasures are being taken to allow processing of classified material. Commanding Generals can accredit systems at SECRET and below.

a. Accreditation Process. Without proper accreditation no computer system will process classified or sensitive material. The accreditation process is as follows:

(1) Prepare the ADP Security Survey (appendix C).

(2) Conduct a Risk Assessment in accordance with OPNAVINST 5239.1H and appendix D.

(3) Prepare a line diagram showing the physical layout of the controlled space where the equipment resides, general building layout, and area layout.

(4) Develop an ADP security SOP and contingency plan. It will be forwarded to the Security Manager for approval and will be part of the documentation maintained and used by the section.

(a) The security SOP will be prepared to outline internal security procedures and will, at a minimum, list hardware and software serial numbers; physical, data, personnel and software control measures; and results of accreditation and TEMPEST survey, when completed.

(b) The contingency plan will be prepared to ensure correct procedures and continued operation in the case of lost or modified data, lost or damaged equipment, sudden personnel turnover, or emergency destruction of ADP media and data.

(5) Initiate the TEMPEST Vulnerability Assessment Request (TVAR) using appendix E as a guide. A waiver shall be requested to ensure the activity can continue to process data while awaiting the TEMPEST survey. Ensure that the appropriate safeguards are in place for security of ADP media.

(6) The Security Survey, Risk Assessment, TVAR, ADP SOP and Contingency Plan will be forwarded to the security manager for comment and consideration. These documents will then be forwarded to the Commanding General for approval. Upon approval, a Statement of Accreditation will be forwarded from the Commanding General to the appropriate staff section.

(7) The Commanding General, represented by the Security Manager, is the Designated Approval Authority (DAA) for accrediting activities processing up to and including SECRET material. Accreditation packages requesting processing authority for TOP SECRET or higher data will be forwarded to the CMC (Code CCIE). After reviewing the accreditation support documentation, A Statement of Accreditation (appendix F) will be issued to the activity or the documentation will be returned for further work and resubmission.

(8) While awaiting accreditation, the requester will initiate security training. Follow on training will be in accordance with appendix B.

b. Tempest Vulnerability Assessment Request (TVAR). Requests for accreditation must be accompanied by a TVAR which is submitted to the Naval Security Group in accordance with OPNAVINST C5510.93E. The TVAR request should be submitted using appendix E as a guide. In the request, a waiver should be requested to prevent having to wait for the survey. The IBM Displaywriter, TEMPEST Z-150/200, TEMPEST Grid Computer, and other TEMPEST accredited computers do not require submission of a TVAR.

4. OPERATION OF ADP EQUIPMENT PROCESSING CLASSIFIED INFORMATION.

a. When processing classified information using computer equipment, the user must process in the "system high mode". Access to the system will be limited to personnel with the clearance, access and "need-to-know" for the highest level of material accessible by the system. When people who lack the clearance or access are in the vicinity of a computer processing classified data, the operator will cease processing until the area is clear. UNDER NO CIRCUMSTANCE WILL A COMPUTER PROCESSING CLASSIFIED INFORMATION BE LEFT UNATTENDED.

b. For those systems accredited to process classified information, the following rules apply:

(1) The system will be afforded the level of protection required for the highest classification of data being processed.

(2) If processing classified material on a system with an integral hard disk drive, the entire system must be treated as a classified document. The system is now the same as an open safe. Unless such protection can be provided, systems with integral hard disks will be used only for unclassified processing.

(3) The magnetic media used for processing classified information will be clearly marked and be in compliance with existing directives.

(4) Each system component must be powered on and off at least three times before processing information of a different classification, such as changing from system high SECRET to system high CONFIDENTIAL. To prevent damage to equipment the user will power off for at least 60 seconds and power on for at least 60 seconds. Using shorter time intervals may damage the equipment.

(5) No computer system connected to any unclassified data communication system (i.e., modem, LAN, WAN, DDN, MCDN, etc.) shall be used to process classified material, unless the modem output is encrypted (e.g., KG-84).

5. SOFTWARE SECURITY.

a. Vendor Supplied Applications. Vendor applications packages such as Wordstar, dBase III and SuperCalc are delivered to the user on diskettes and are clearly marked. These packages will be stored in a suitable container. No additional markings will be required on vendor supplied diskettes. These diskettes will be treated as unclassified. These diskettes should be backed up and protected. Unauthorized copies of vendor supplied applications, e.g., for personal use, must not be made as such action may constitute a violation of copyright laws.

b. Class II Applications. Locally developed applications (Class II) programs will be stored on unclassified diskettes. These programs will be clearly marked as unclassified.

c. Freeware/Shareware/Games. Due to the attacks of virus programs many organizations have suffered significant loss of programs/data. Virus-ridden programs are usually retrieved from electronic bulletin board services by using a computer and modem to connect to the service and download a program. Programs retrieved in this manner or passed between friends/associates are expressly forbidden on government equipment. A simple rule

applies: If the program was not purchased through approved government procurement channels DO NOT USE IT! Each Commanding General is granted waiver authority for use of shareware and freeware.

d. Write Protect Tabs. All diskettes containing vendor software will be write protected before inserting into a computer which processes classified material. This involves placing a write protect tab over the write protect notch on the side of the diskette. This will prevent unintentional writing of classified data to an unclassified diskette. This requirement also applies to diskettes containing data of a lower classification than that being processed on a system (i.e., a user may not place an UNCLASSIFIED diskette in a computer without a write protect tab while that computer is in a system high mode of SECRET).

6. PHYSICAL SECURITY.

a. Access Control. Positive physical access controls must be established to prevent unauthorized entry into the controlled space. A list of all personnel authorized to operate microcomputers/workstations shall be posted close to each device. The list will contain name, clearance of authorized users and the name and phone number of assigned security personnel.

b. System Security.

(1) All systems will be physically secured at all times.

(2) All system components (CPU and all attached peripherals) will be labeled with the highest classification of data authorized to be processed. The label will be visible to the operator and not easily removable.

(3) All systems will have a security checklist displayed in the system work area clearly visible to the operator at all times. A sample format is contained in appendix G. The security checklist outlines the system security procedures before, during, and after processing. All sections will ensure the security checklist is completed at the end of each day or when leaving the controlled space.

c. Monitor Position. All computer video monitors used to process sensitive or classified material will be turned away from any exterior window/door opening. Monitors will be covered (or dimmed) when personnel without proper clearance enter the processing area.

d. Password Control. It is recommended that all microcomputers be password protected. Passwords within a section should be generated, compiled and stored on one slip of paper. This paper should be stored in a combination change envelope. If used,

computer system passwords shall be changed at least as often as security container combinations using a unique mix of six upper/lower case characters/numerics, e.g., J=@x#7. This password must be entered upon initial entry to the system.

e. Logon Warning. All microcomputers will display a warning logo on the screen upon initial entry to the system. This logo will contain the following message:

WARNING ** CAUTION ** WARNING ** CAUTION ** WARNING ** CAUTION

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND/OR SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474.

Public Law 99-474, Title 18, United States Code states that, "Unauthorized access to this United States Government Computer System and software is prohibited by Public Law 99-474, Title 18, United States Code. Public Law 99-474, Chapter XXI, Section 1030 states that, "Whoever knowingly..., or intentionally accesses a computer without authorization, or exceeds authorized access, and by means of such conduct,...obtains..., alters, damages, destroys, or discloses information..., or prevents authorized use of data or a computer owned by or operated for the Government of the United States...shall be punished (by)...a fine under this Title or Imprisonment for not more than 10 years, or both." Report unauthorized use or access to the designated Information System Security Officer or ADP Security Officer."
REPORT UNAUTHORIZED USE OR ACCESS TO THE SYSTEMS SECURITY OFFICER.

WARNING ** CAUTION ** WARNING ** CAUTION ** WARNING ** CAUTION

This warning, when flashed on the screen, must force the user to press some key or take some action to clear the screen of the message. The command ISMO maintains the capability to implement this policy.

f. Random Sampling of Data Disks. Each week ADPSOs/ADPSSA's will randomly verify the contents of working disks to ensure that they contain no data higher than the stated classification level. Working disks which are not used on a daily basis will have write protect tabs placed on them to ensure that classified data is not inadvertently placed on them.

7. DATA SECURITY.

a. Floppy diskettes.

(1) All 8, 5.25, and 3.5 inch floppy diskettes will be color coded and clearly marked according to the highest classification of the data on them. The diskette jacket (mylar plastic envelope containing the floppy magnetic medium) will be colored in its entirety according to the following color codes:

UNCLASSIFIED - Black, Green, Gray, or White
CONFIDENTIAL - Blue
SECRET - Red
TOP SECRET - Orange
SCI - Yellow

(2) The Classified Material Control Center (CMCC) will order, account for, and distribute color coded diskettes used for classified information (less SCI/yellow diskettes). Diskettes should be received by the CMCC in heat shrunk packaging. After the heat seal has been broken, all diskettes will be logged and accounted for by the CMCC and afforded the protection required for a document of the appropriate classification. This accounting control is required even if the diskettes are blank. Information placed on the diskette jacket (not the paper sleeve) will include a control number, dissemination control information, the owning organization and compartments/codewords (where applicable). This information will be written on the diskette using an indelible marker. Ball point pens will not be used because of the potential damage to the floppy disk magnetic medium. When diskettes are returned to the CMCC for storage, a current, dated listing of all files contained on the diskette will be included.

(3) Only the Special Security Officer (SSO) is authorized to order and stock SCI (yellow) diskettes. All SCI diskettes will be numbered and accounted for by the same procedures outlined in the above paragraph. At no time will any diskette be removed from the SCIF without the written approval of the SSO.

(4) If color coded diskettes are not available, the diskette used will be prominently marked with the highest classification of data stored on it and will comply with all other security requirements of this order. This is an interim measure until such time that appropriately colored diskettes can be obtained. Once acquired, the data will be transferred to the appropriate colored diskette and the old disk will be destroyed.

(5) Vendor supplied application packages, which are unclassified and are not black, green, white, or gray are authorized and do not require conversion to those colors.

b. Hard Disk Drives/Cartridges. Many microcomputers have removable hard disk drives/cartridges. When classified material is processed on these drives, the entire cartridge/drive is then considered classified and should be treated as such. During the time the cartridge/drive is in the machine, the entire machine is considered classified and appropriate precautionary actions must be taken to insure its security. Hard disk cartridges/drives with classified material will be clearly marked to include the highest classification of data stored, protected, and physically secured at all times. They will be removed and stored in appropriate

security containers when not in use. Additionally, the serial number of the cartridge/drive will be identified and kept on record for accountability as containing classified data.

c. Integral Hard Disk Drives. Devices with integral hard disk drives (hard disk drives that are not removable) should not be used to process classified information. However, if no alternative exists then the entire system must be protected, marked and physically secured at all times at the level afforded the highest classification of data ever processed on the system. Additionally, these systems must be identified by serial numbers to ensure that the drive is accounted for even when maintenance is performed.

d. Other Media. All other removable media (cassette tape, paper tapes, etc.) which contain classified data will be accounted for in accordance with the highest classification of data that they have ever contained. SCI data will be stored by the SSO when not in a security container or in the CMCC when not in use. All classified media when returned to the Secondary Control Point (SCP), CMCC or SSO will contain a current, dated listing of all filenames contained on that media.

8. DESTRUCTION OF CLASSIFIED DATA STORED ON MAGNETIC MEDIA.

a. Floppy Diskettes. Diskettes will not be downgraded or declassified. The only authorized disposal methods for diskettes are incineration or shredding.

b. Hard Disk Drives/Cartridges.

(1) Reusable. Hard disk drives/cartridges used to process classified material can be wiped clean and reused for unclassified data. This is accomplished by the execution of an approved program for declassification of magnetic media which can be obtained from the command ISMO. If a hard drive/cartridge used to process classified material requires maintenance, it will first be screened by the ISMO. If it is determined that the drive is repairable, the ISMO will take steps to return it to operating condition. If the drive/cartridge must be removed from the site for repair, it will be wiped clean by an approved program for declassification of magnetic material. If this cannot be accomplished, the drive must be destroyed as defective.

(2) Defective. Hard disks containing classified data will be physically destroyed by smashing the external casing, running a powerful magnet over the magnetic platter(s) and scrubbing the platters with an abrasive, steel wool pad. Destruction will be recorded in a destruction report to the CMCC or SSO, as appropriate.

c. Random Access Memory (RAM). RAM is the transient memory in the central processing unit of a computer. This memory is only

active when power is supplied to the system. After classified data has been processed, and before data of any other classification level can be processed, RAM must be cleared of all data. This will be accomplished by following the instructions in paragraph 4.b.4 of this order.

d. Complimentary Metal Oxide Semiconductor (CMOS). Another form of memory which exists in many laptop systems is CMOS memory. This type of memory does not lose its contents when powered off. When this type of memory exists in a machine that processes classified material, a program must be executed to write unclassified data (static 1's) into the memory before the machine is powered down. If the unit cannot be brought up to accomplish this task, the machine must be physically secured and handled as a classified document equal to the highest level of material processed thereon.

9. TRANSMISSION EQUIPMENT/CLASSIFIED DATA.

a. No transmission equipment (e.g., modems) will be connected to ADP equipment processing classified data unless approved in writing by the DAA.

b. Local Area Networks (LANs). No classified data will be processed on microcomputers connected to a LAN until approval is received in writing from the DAA. If one computer on a LAN contains classified material, every machine on that LAN is considered classified and appropriate precautionary actions should be followed. These guidelines also apply to microcomputers established on a wide area network (WAN).

10. PRIVATELY OWNED MICROCOMPUTERS. Privately owned microcomputers are not allowed in workspaces.

GLOSSARY

A. Accreditation. A policy decision by the responsible DAA resulting in a formal declaration that appropriate security countermeasures have been properly implemented for the ADP system and that the system is operating within an acceptable level of risk.

B. Automatic Data Processing Equipment for the Fleet Marine Forces (ADPE-FMF). Ruggedized IBM Series 1 computer equipment used to process Class IA Systems. Commonly known as the "Green Machine".

C. Compromising Emanations. Unintentional data relayed or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information being received, handled or otherwise processed by ADP equipment. See TEMPEST.

D. Contingency Plan. A plan for emergency response, backup operations, and post-disaster recovery maintained by an ADP activity as part of its security program.

E. Controlled Space. The three-dimensional space surrounding equipment that processes classified information within which unauthorized personnel are either denied unrestricted access or escorted by authorized personnel and are under continual surveillance. If the equipment is used only to process unclassified information, it is the area set aside for the equipment. Controlled Space should not be confused with Controlled Area which applies to the establishment of Restricted Areas.

F. Data Media. The medium on which data is processed, stored or otherwise manipulated. It includes, but is not limited to, diskettes, hard disk, magnetic tape, paper tape, paper, memory and monitor.

G. Degauss. To apply a variable, alternating current field for the purpose of demagnetizing magnetic recording media.

H. Designated Approving Authority (DAA). An official assigned responsibility to accredit ADP activities.

I. End User Computers (EUC). Generic name for personal computers, microcomputers or minicomputers. Examples are IBM PC, Zenith 248 and 150, Grid and Televideo.

J. Fleet Marine Force-End User Computing Equipment AN/UYK-83 (FMF-EUCE). Ruggedized microcomputer equipment to replace the ADPE-FMF equipment (Green Machine).

K. Hard Disk Drive. A rigid device for magnetic data storage. Hard disks provide data storage of 10 megabytes or more.

1. Hard disk drive/cartridge: Removable disk drive/cartridge that allows for disk/cartridge storage of classified information separate or away from a computer system.

2. Integral/fixed hard disk: Hard disks that are internal to the computer system and are not removable for separate data storage purposes. Integral/fixed hard disks are not to be used for classified processing.

L. Modem. Modulator/demodulator. A communication device commonly connected to computers for data transmission.

M. Password. An electronic signature used to gain operator access to a computer system. Normally a combination of letters, numbers, and special characters much like the combination to a safe.

N. TEMPEST. An unclassified term referring to investigations and studies of compromising emanations.

O. TEMPEST-accredited ADP equipment. Equipment which is designed and meets a stringent set of laboratory TEMPEST standards based on qualification testing and can be installed in almost any environment without presenting a TEMPEST problem. The manufacturer guarantees to support the TEMPEST posture of these devices. Example is Zenith Z150.

P. TEMPEST-approved ADP equipment. Equipment which is not designed for TEMPEST but meets a selected set of minimum TEMPEST requirements based on statistical evaluation of field or laboratory testing and can be installed in certain general environments without presenting a TEMPEST problem. The manufacturer will not necessarily maintain the TEMPEST posture of these devices.

Q. Sensitive Material. Any data as covered by the provisions of the Privacy Act Statement of 1974 such as personnel rosters, medical data, and fitness report information; and any data, although unclassified, standing alone, which, when combined with other data would become classified such as morning reports, training reports, logistics summaries, and fiscal information.

R. System High. When a system is processing classified information, only those individuals possessing the requisite clearance for the highest classification of data in the system and possessing the "need-to-know" will be allowed access to the system.

S. Tempest Vulnerability Assessment Request (TVAR). A request submitted to the Naval Security Group to measure computer emanations.

T. Local Area Network (LAN). A wiring configuration (including internal computer expansion cards and computer software) required to connect several microcomputers together over a predefined area.

U. Wide Area Network (WAN). A WAN is similar in definition to a LAN but is distinctly larger in scope. A WAN usually connects several LANs over a widely dispersed geographic area.

TRAINING

1. Commanding officers are responsible for security education within their commands, and for insuring it is afforded a significant share of the time dedicated to command security. Within the security education program, time should be allotted for specific ADP security training.

2. The entire program regarding ADP security education should encompass three areas: orientation, on-the-job training and refresher briefings.

a. Orientation. As soon as possible after reporting, all persons who will be using ADP equipment will be given an orientation briefing concerning proper ADP security procedures. This orientation briefing will encompass general ADP security procedures as well as procedures which may be unique to a particular command. Additionally, the ADPSO and ADPSSA will be identified to all new arrivals.

b. On-the-Job Training.

(1) Supervisors must assure themselves that subordinates know the ADP security requirements impacting on the performance of their duties. Supervised on-the-job training is the phase of ADP security education when application of specific procedures is learned.

(2) Supervision of the on-the-job training process is critical. Not only does supervision leave nothing to chance, it reinforces that the supervisor is genuinely concerned about the protection of classified material processed on ADP equipment. This concern then carries down to the subordinates resulting in enhanced awareness throughout the organization.

c. Refresher Briefings.

(1) Annually, all personnel who use ADP equipment will receive a refresher briefing or equivalent training designed to enhance their ADP security awareness. This briefing is most appropriately given concurrently with the required annual security briefing for personnel who have access to classified material.

(2) This annual refresher briefing does not have to cover the entire area of ADP security. It should at least cover changes in policies or procedures and any particular problem areas which have arisen in the past year. Any refresher briefings may be broken down into separate briefings for supervisory personnel, users and ADPSOs and ADPSSAs.

EUC/OIS ADP SECURITY SURVEY

A. Basic Data. (Applies to all ADP systems)

1. Major Command:_____ Section:_____

   Equipment Name:_____ Work Phone:_____

2. System Identification:_____

   ( ) Office Information System

   ( ) ADP System (PC's and ADPE-FMF)

   ( ) Network

3. System Description: (List all components, computers, peripherals, communications processors, encryption devices, remote devices, network and remote interfaces, etc.)

_____

_____

_____

_____

_____

_____

_____

_____

4. Equipment Location:_____
   Bldg:_____
   Room:_____ Phone:_____

5. System Operations Contact for Security:
   Name:_____
   Code:_____
   Building:_____ Room:_____
   Phone:_____

6. Types of Data Processed

TYPE OF DATA	PERCENT OF PROCESSING TIME
TOP SECRET	
SECRET	
CONFIDENTIAL	
Privacy Act	
For Official Use Only	
Financial	
Sensitive Management	
Proprietary	
Privileged	
Unclassified	
TOTAL	100%

7. Operating System and Standard Applications Software Identifications:

_____

_____

_____

8. Scope of System: (Check all that apply.)

( ) Stand-alone and single controlled space.

( ) Multiple stand-alone and single controlled space

( ) Other: _____

9. Total Value of System: $_____ (Dollar value of impact of loss and cost to replace)

(a) Equipment: $_____

(b) Software: $_____

(c) Data: $_____

10. Mission Related

(a) Primary Function(s) of the System or Network:

_____

_____

_____

(b) Contingency Plan Requirement:

( ) Plan is in existence. Date of plan is _____

( ) Plan is being developed. Estimated completion date is _____.

( ) Plan is not required because loss of processing capability for a reasonable period of time would not adversely affect mission. (For example 2, 4, 8 hours, 2 days, etc. depending on the criticality of the ADP function.) Provide justification.

B. Site Security Profile and Minimum Requirements for Environmental and Physical Security.

1. Vulnerability: Temperature or Humidity Outside Normal Range. Operating Countermeasures: (Check all that apply.)

( ) Adequate heating and controls
( ) Adequate cooling and controls
( ) Only designated personnel operate controls
Other:_____

Assessment of Risk:
( ) High ( ) Moderate ( ) Low

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

( ) Adequate primary lighting
( ) Adequate emergency lighting
( ) Adequate periodic checks of emergency lighting
( ) Adequate primary power and outlets
( ) Functioning power filters or voltage regulators
( ) Available backup power
( ) Other:_____

Assessment of Risk:
( ) High ( ) Moderate ( ) Low

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

( ) Routine cleaning schedule is adhered to
( ) Smoking, eating, and drinking are not permitted in equipment areas
( ) Other:_____

Assessment of Risk:
( ) High ( ) Moderate ( ) Low

4. Vulnerability: Unauthorized Physical Access. Operating Countermeasures: (Check all that apply.)

( ) Perimeter fence
( ) Security guards
( ) Building secured outside of normal working hours
( ) Area alarms (motion detectors, open door detectors, perimeter penetration detectors)
( ) Authorized access list
( ) Cipher door lock
( ) Combination door lock
( ) Recognition of authorized personnel
( ) Closed circuit television
( ) Administrative procedures
( ) Physical isolation/protection
( ) High employee morale
( ) Close supervision of employees
( ) Indoctrination of personnel
( ) Security awareness
( ) Security devices (desk anchor pads, etc.) used
( ) EUC/OIS not installed in high traffic areas
( ) Controlled space
( ) Other:_____

Assessment of Risk:
( ) High ( ) Moderate ( ) Low

5. Vulnerability: Software/Data Protection. Operating Countermeasures: (Check all that apply.)

( ) Data properly stored, accessed,handled and marked
( ) Data media (diskettes, hard disk, output) properly stored and handled
( ) Contractor supplied software properly stored and handled
( ) Contractor supplied software assigned to specific EUC/OIS

( ) Unauthorized copies of contractor supplied software being produced and used
( ) Other: _____

Assessment of Risk:
( ) High ( ) Moderate ( ) Low

C. Current status of accreditation support documentation. (Applies to all EUC activities and networks which will be authorized to handle classified).

1. All ADP activities and networks which will be authorized to handle classified data must either be accredited or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation. This section provides a statement of the current status of the accreditation support documentation.

				In Existence
				Being Developed
				Required but no action taken
				Not Required
( )	( )	( )	( )	Security Standard Operating Procedures Handbook
( )	( )	( )	( )	Line diagrams showing interconnection of components and physical layout and networks
( )	( )	( )	( )	Copies of previous accreditation
( )	( )	( )	( )	TEMPEST accreditation request
( )	( )	( )	( )	Risk Assessment
( )	( )	( )	( )	Other (specify): _____

D. Survey Data.

1. Current Status: _____

2. Survey Prepared By:
Name: _____
Code: _____ Bldg: _____
Room: _____ Phone: _____

To the best of my knowledge, the information provided in this survey and the attached documentation is complete and accurate.

Signature: _____
Date: _____

RISK ASSESSMENT

A. INTRODUCTION. Risk is derived from the evaluation of threats and vulnerabilities in relationship to the assets of the ADP activity. This evaluation forms the basis for action to manage the risk by identifying effective countermeasures.

B. PREPARATION OF RISK ASSESSMENT. For those activities processing classified data a risk assessment will be forwarded with the ADP Security Survey as part of the accreditation package. Subparagraphs (1) through (4) below will be repeated for each identified threat.

(1) Threat Identification. A threat is any agent capable of reducing the effectiveness of an ADP activity. Threats can be natural or man-made, deliberate or accidental. Examples of these threats are: natural disasters (fires, flood, earthquake), authorized users (programmers, operators, customers, maintenance personnel) and anyone who is not an authorized user.

(2) Vulnerability Analysis. A vulnerability is a weakness that could be exploited by a threat agent to cause harm to the ADP activity. Examples of vulnerabilities are geographical location, security modes of operation, level and volume of data being handled, and overall criticality of the ADP operation.

(3) Risk Assessment. Possibility of certain threat to exploit a vulnerability. Risk is expressed as Low, Moderate, or High.

(4) Countermeasure(s) Identification. Identifying measures that could be taken by the activity to remove or reduce the risk of the threat and/or vulnerability to the ADP system.

TEMPEST VULNERABILITY ASSESSMENT REQUEST

A. INTRODUCTION. Any activity which uses EUCE for classified processing will submit a Tempest Vulnerability Assessment Request (TVAR) with its accreditation package.

B. PREPARATION. The TVAR will contain all the information requested below to ensure that a proper TEMPEST scheduling priority can be established by the certifying unit. When a tentative date for the survey is set, the requesting activity will be notified at least two weeks prior to the start of the survey. In some cases, a survey will not be performed; the requesting activity will be sent a waiver allowing it to process classified information.

1. TVARs will be addressed as follows:

To: Commander Naval Security Group (Code G65)
Washington, D.C. 20390

Via: Applicable Chain of Command
Commanding General
Fleet Marine Force, Pacific/Marine Corps Bases, Pacific (C3B/OP)
Camp H. M. Smith, Hawaii 96861-5001

Copy to: Chief of Naval Operations
(OP-009P)
Washington, D.C. 20390

Commanding Officer
(Code 220)
Naval Electronics System Security Engineering Center
3801 Nebraska Avenue, N.W.
Washington, D.C. 20390

Commanding Officer
Naval Electronics System Engineering Center, San Diego (Code 34)
P.O. Box 80337
San Diego, CA 92138

Commandant of the Marine Corps
(Code CCTO)
Headquarters, U. S. Marine Corps

Washington, D.C. 20380-0001

2. TVARs will contain the following information:

Subj: INSTRUMENTED TEMPEST SURVEY (ITS) REQUEST

Ref: (a) OPNAVINST C5510.93
(b) (Report of last Instrumented TEMPEST Survey)

Encl: (1) Facility Layout/Floor Plan/Elevation Views

1. (U) In accordance with reference (a), we are submitting a TEMPEST Vulnerability Assessment Request (TVAR) for (System, Equipment) located at (Building No., Base, City, State). The following information is provided, in accordance with Section III, enclosure (2) of reference (a):

a. (U) Reporting Unit Code (RUC):

b. (U) System/Equipment: (Provide a general description of the system/equipment to be tested.)

c. (U) List of Equipment: (Provide a list of equipment to be tested including individual component nomenclature, model number, and quantity of all equipment which will process classified information.)

d. (U) Floor Plans and Vertical Equipment Configuration Drawings (see enclosure (1)): (Provide sketches of the facility layout and floor plans/elevation views showing location of the classified processors.)

e. (U) List of equipment changed since last ITS: (Listing of the specific equipment or systems deleted, added, or relocated since last Instrumented TEMPEST Survey or Vulnerability Assessment.)

f. (U) System/Equipment was installed by: (Identification of installing activity, i.e., station/ship's forces, outside activity (identify the outside activity)).

g. (U) System/Equipment is a (high/low) level installation. State whether the equipment operates low level (i.e., +/-6 volts DC signaling in accordance with MIL-STD-188) or high level and ADPSP EUC/OIS indicate if the installation is in accordance with approved installation plans. Identify the approved plans.)

h. (U) Amount of traffic/data processed:

(1) Total Volume -_____-printed pages/month or screens of video display terminal data/month.

(2) Highest classification processed is:_____

(3) Unclassified Percentage:_____

(4) CONFIDENTIAL Percentage:_____

(5) SECRET percentage:_____

(6) TOP SECRET Percentage:_____

(7) Sensitive Compartmented Information (SCI):_____

i. (U) Power Source: The system/equipment is fed by (filtered/unfiltered) (commercial/government) AC power system. A power transformer is located (inside/outside) controlled area.

j. (U) Minimum Controlled Space: Minimum distance between the system/equipment and closest area where hostile compromising emanations intercept efforts may occur; i.e., the minimum controlled space distance is _____ meters away. (Consider the areas above and below the equipment or systems. Also, indicate location on the facility layout.)

k. (U) This is the first survey request for the newly installed equipment or the system was last tested during (dates) and the survey results were reported by reference (b).

l. (U) Point of Contact: The point of contact at this activity is (name) at AUTOVON (phone number).

m. (U) Remarks: (Include all amplifying information that could assist in determining hazard probabilities or priority of TEMPEST survey.)

(Note: This entire sample letter is unclassified. If classified data is entered in paragraph l., h. or m. then appropriately classify these paragraphs.)

STATEMENT OF ACCREDITATION

From: Commanding General
To: _____

Subj: SECURITY ACCREDITATION OF (Name of Section)

Ref: (a) OPNAVINST 5239.1A
(b) MCO P5510.14
(c) Accreditation support documentation

1. In accordance with the provisions of references (a) and (b), I hereby accredit the (name of the system). This accreditation is based upon a review of the information provided in reference (c). This accreditation is my formal declaration that appropriate ADP security countermeasures have been properly implemented and that a satisfactory level of operational security is present. This EUC/OIS activity is authorized to process data up to _____ in the system high security mode of operation.

2. This accreditation is valid for five years from the date of this letter or sooner if there is a change affecting the security posture of the activity. It is your responsibility to ensure that any change in configuration, mode of operation, or other modification is evaluated to determine its impact on ADP security and that appropriate action is taken to maintain a level of security consistent with the requirements for this accreditation.

3. A copy of this accreditation letter with supporting documentation will be retained by the activity as a permanent record.

CG (SIGNATURE)

Note: If there are several EUC/OIS activities in one command/ staff section list them in an enclosure providing data level and security mode of operation.

ForO 5239.1
29 Apr 90

SECURITY CHECKLIST

PRIMARY OPERATOR: _____

OTHER AUTHORIZED OPERATORS: _____

Before Processing:

1. Ensure operator clearance for material. Ensure no unauthorized personnel are within viewing range of the monitor.

2. Ensure operator is using the proper colored diskette.

3. Ensure the system is in the appropriate SYSTEM HIGH MODE. If changing between different modes clear the system as described below.

During Processing:

1. Never leave classified data unattended.

2. Dim monitor when personnel without clearance or need-to-know enter area.

3. Produce listing of disk contents on all level I data.

4. If leaving the area, exit program, clear screen, and possibly reengage password lock (RELOCK).

5. Never write, even temporarily, to the HARD DISK.

After Processing Classified Data:

1. Clear system by following these steps:

TURN SYSTEM OFF-WAIT 1 MINUTE
TURN SYSTEM ON -WAIT 1 MINUTE
TURN SYSTEM OFF-WAIT 1 MINUTE
TURN SYSTEM ON -WAIT 1 MINUTE
TURN SYSTEM OFF-WAIT 1 MINUTE
NO SHORTCUTS!

2. Ensure all floppy disks are removed from computer.

3. Ensure all diskettes/listings are in appropriate containers.

Appendix G to
ENCLOSURE (1)

4. Ensure all impact printer ribbons are removed and properly stored.

5. Ensure all systems and components are powered down.

IF YOU HAVE ANY QUESTIONS, CONTACT THE ADPSSA

ADPSSA:_____ ADPSO:_____